hw

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/843,760	04/30/2001	Lawrence M. Besaw	10006612-1	9179

7590 12/22/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
CHANKONG, DOHM	
ART UNIT	**PAPER NUMBER**
2152	

DATE MAILED: 12/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/843,760	**Applicant(s)** BESAW, LAWRENCE M.	
	Examiner Dohm Chankong	**Art Unit** 2152	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 30 December 1899.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 21-53 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 21-53 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1> This action is in response to Applicant's remarks, filed 10.18.2005. Claims 21-53 are presented for further examination.

2> This is a non-final rejection.

Response to Arguments

3> Applicant's arguments, with respect to the rejection(s) of claim(s) 21-52 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of new prior art as set forth below.

4> Paragraph 12 of Applicant's remarks discuss the authentication capabilities of Lim and assert that

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5> Claims 21, 22, 26-28, 30, 32, 37, 38, 41-43, 45, 47, 52 and 53 are rejected under 35 U.S.C § 103(a) as being unpatentable over Lim et al, U.S Patent No. 6.434.619 ["Lim"], in view of Hutcheson et al, U.S Patent Publication No. 2003|0032409 ["Hutcheson"].

6> As to claim 21, Lim discloses a method for filtering on-line service information provided through a management portal to a customer of customized network services provided by resources of a service provider network, comprising:

applying a display filter to resources of the server provided network, said display filter specifying network resources for which the on-line service information is desired by the customer [column 4 «lines 46-66» | column 10 «lines 51-59»]; and

executing at least one management information module to generate a portal display of on-line service information, wherein said at least one management information module operates on only those network resources of said service provider network which have not been excluded by said display filter [column 5 «lines 1-32» | column 10 «lines 24-59»].

Lim does not explicitly disclose utilizing a security filter.

7> Lim does disclose utilizing authentication measures to allow a user access only to his directory (partitioned storage) [column 9 «lines 24-27 and lines 53-57»] and then applying appropriate filters [column 10 «lines 43-59»] after the user has been authenticated. But as mentioned previously, Lim does not explicitly disclose a security filter definable by the service provider, not the customer. In the same field of invention, Hutcheson is directed towards a system for distributing content to subscribers. Hutcheson discloses applying to said service provider network a security filter definable by service provider and not the customer, said security filter corresponding to the customer and specifying the network resources allocated to that customer [0164, 0193 where : the administrator defines the privileges for each group and user, the privileges restricting their access to specified resources]. It would have been obvious to one of ordinary skill in the art to incorporate Hutcheson's security (privilege) filter into Lim's management system to provide the administrator control over who is capable of accessing and viewing network resources [see Hutcheson, 0163].

8> As to claim 22, Lim and Hutcheson disclose a method wherein applying said security filter comprises:

applying a customer sub-filter to provide an association of said corresponding customer and said network resources contained in said partitioned network allocated to the customer [see Lim, column 9 «lines 18-27» | column 10 «lines 24-42» : "...data associated with the customer are polled by the system..."].

9> As to claim 26, Lim discloses a method for filtering on-line service information presented through a management portal to a customer of customized network services provided by resources of a service provider network, comprising:

partitioning the service provider network into a plurality of partitioned networks [column 1 «lines 30-51» | column 3 «lines 22-29»];

allocating one of said partitioned networks to the customer [column 1 «lines 36-51» |

column 20 «lines 61-62» | column 21 «line 28»];

providing a plurality of modules each configured to provide a respective portal display of on-line service information [column 4 «lines 46-51»];

storing, in a filter library accessible to the customer, of display filters each configured to specify customer-selected network resources to which selected ones of said plurality of modules is to be applied [column 4 «lines 46-66» | column 10 «lines 51-59»]; and

displaying a portal display of on-line service information generated from application of one of said plurality of modules to network resources resulting from application to the service provider network of at least one of said display filters [column 5 «lines 1-32» | column 10 «lines 24-59»].

Lim discloses a configuration database [column 7 «lines 56-60»] but does not explicitly disclose security filters or storing them in the configuration database accessible by the service provider and not the customer.

10> Lim does disclose utilizing authentication measures to allow a user access only to his directory (partitioned storage) [column 9 «lines 24-27 and lines 53-57»] and then applying appropriate filters [column 10 «lines 43-59»] after the user has been authenticated. But as mentioned previously, Lim does not explicitly disclose a security filter. In the same field of invention, Hutcheson is directed towards a system for distributing content to subscribers. Hutcheson discloses applying to said service provider network a security filter definable by service provider and not the customer, said security filter corresponding to the customer and specifying the network resources allocated to that customer [0164, 0193 where : the administrator defines the privileges for each group and user, the privileges restricting their access to specified resources]. It would have been obvious to one of ordinary skill in the art to incorporate Hutcheson's security (privilege) filter into Lim's management system to provide the administrator control over who is capable of accessing and viewing network resources [see Hutcheson, 0163].

11> As to claim 27, Lim and Hutcheson disclose a method wherein applying said security filter comprises:

applying a customer sub-filter to provide an association of said corresponding customer and said network resources contained in said partitioned network allocated to the customer [see Lim, column 9 «lines 18-27» | column 10 «lines 24-42» : "...data associated with the customer are polled by the system..."].

12> As to claim 28, Lim discloses a customer sub-filter that is configured to filter on at least one of a node level and interface level of said service provider network [column 4 «lines 52-62» | column 5 «lines 1-24» : see Lim's interfaces].

13> As to claim 30, Lim discloses specifying an internet protocol interface sub-filter of said security filter, said IP interface sub-filter configured to filter on an IP address of a network device [column 5 «lines 1-24»].

14> As to claim 32, Lim discloses the method of claim 26 further comprising specifying an interface selection sub-filter of said display filter, said interface selection sub-filter configured to filter one of a set of at least one network interfaces [column 10 «lines 24-59»].

15> As to claim 37, Lim discloses providing a network health module configured to display a status or health report network resources to which said network health module is applied [column 1 «line 63» to column 2 «line 3» | column 5 «lines 46-55»].

16> As to claim 38, Lim discloses storing a network health sub-filter of the display filter, said network health sub-filter configured to identify which of said network elements to monitor for said status and health report [column 6 «lines 13-32»].

17> As to claim 40, Lim discloses invoking said display filter by invoking said selected module [column 5 «lines 7-32»].

18> As to claims 41-43, 45, 47, 52 and 53, as they are merely systems that implement the steps of the method of claims 26-28, 30, 32, 37 and 38, they do not teach or further define over the claimed limitations. Therefore, claims 41-43, 45, 47, 52 and 53 are rejected for the same reasons as set forth for claims 26-28, 30, 32, 37 and 38, supra.

19> Claims 29, 39 and 44 are rejected under 35 U.S.C § 103(a) as being unpatentable over Lim and Hutcheson, in further view of Teijido et al, U.S Patent No. 2002|0053020 ["Teijido"].

20> As to claim 29, Lim and Hutcheson do disclose utilizing sub-filters [see Hutcheson, 0143, 0164 : privilege filters accessible resources, profile further refines accessible resources to ones of interest to the user] but do not explicitly disclose specifying an internet protocol host sub-filter of said security filter, said IP host sub-filter configured to filter on a network name of a network device.

21> Teijido discloses an internet protocol host sub-filter of said security filter, said IP host sub-filter configured to filter on a network name of a network device [0049, 0070 : "...limit access to only a predefined specific set of client machines."; "...host id"]. It would have been obvious to one of ordinary skill in the art to incorporate Teijido's host sub-filter into Lim's management system to provide a level of security in accessing and viewing network resources. Such an implementation would ensure that the data can be tailored to a specific set of client machines.

22> As to claim 39, Lim does not explicitly disclose invoking said security filter by parsing a customer record in said user configuration database.

23> Teijido discloses invoking said security filter by parsing a customer record in said user configuration database [0105, 0111 where: Teijido discloses checking a user's ASP]. It would have been obvious to one of ordinary skill in the art to implement Teijido's user verification functionality into Lim's management system to correlate a user with the documents or information that he is allowed to access. Such an implementation would provide increased security in Lim's system by preventing users from accessing information that they are not allocated.

24> As to claim 44, as it does not teach or further define over the previously claimed limitations, it is rejected for the reasons set forth for claim 29, supra.

25> Claims 23-25, 31, 33-36, 46 and 48-51 are rejected under 35 U.S.C § 103(a) as being unpatentable over Lim and Hutcheson, in further view of Rangarajan et al, U.S Patent No. 6.275.225, ["Rangarajan"].

26> As to claim 23, Lim and Hutcheson do not explicitly disclose an alarm module.

27> Rangarajan discloses an alarm module configured to display information regarding alarm conditions occurring in said non-excluded resources [Figure 5 «item 509» | column 5 «lines 50-53» | column 10 «lines 6-10» : wherein the devices correspond to network resources and clients are only able to work with resources that have been assigned to them (excluded resources)]. Furthermore, Lim discloses resources that can only be utilized by customers with the property authority. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's alarm module into Lim's management system to allow users to select nodes that would enable monitoring of alarm conditions in the network resources to which they only have access. One would have motivated to perform such an implementation enable users to more efficiently manage resources.

28> As to claim 24, Lim and Hutcheson do not explicitly disclose a topology module configured to display at least a graphical representation of network elements and connections between said network elements included in said non-excluded network resources.

29> Rangarajan discloses providing a topology module configured to display at least a graphical representation of network elements and connections between said network elements [Figure 9 «item 905» | column 6 «lines 27-36» | column 7 «lines 21-24»]. Furthermore, Lim discloses resources that can only be utilized by customers with the property authority. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's topology module into Lim's management system to allow users to more clearly see a map of the configuration of network resources to which they only have access in the network. One would have been motivated to perform such an implementation as such a map would allow users to more effectively manage the network resources.

30> As to claim 25, Lim and Hutcheson do not explicitly disclose a network health module configured to display a status or health report of said non-excluded network resources.

31> Rangarajan discloses a network health module configured to display a status or health report of said non-excluded network resources [Figure 9 «item 907» : "critical, major, minor.."]. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's health module into Lim's data access system to allow users to keep track and remotely monitor network resources as needed.

32> As to claim 31, Lim and Hutcheson do disclose utilizing sub-filters [see Hutcheson, 0143, 0164 : privilege filters accessible resources, profile further refines accessible resources to ones of interest to the user], but do not explicitly disclose a node selection sub-filter.

33> Rangarajan discloses a node selection sub-filter of said display filter, said node selection sub-filter configured to filter on network nodes of the service provider network [column 6 «lines 27-33» | column 7 «lines 10-14»]. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's node filtering functionality into Lim's management system to enable users to manage network devices through a user selected view of the nodes in the network.

34> As to claim 33, Lim and Hutcheson do not explicitly disclose an alarm module.

35> Rangarajan discloses an alarm module configured to display alarm conditions in network resources to which said alarm module is applied [Figure 5 «item 509» | column 10 «lines 6-10» : wherein the devices correspond to network resources]. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's alarm module into Lim's management system to allow users to select nodes that would enable monitoring of alarm conditions in the network resources. One would have motivated to perform such an implementation enable users to more efficiently manage resources.

36> As to claim 34, Lim and Hutcheson do not explicitly disclose an alarm sub-filter.

37> Rangarajan discloses storing an alarm sub-filter of the display filter, said alarm sub-filter providing filtering capability of a display of alarm categories [column 6 «lines 27-36» | column 7 «lines 37-61»: "selected fault list"]. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's alarm sub-filter into Lim's management system to enable users to select specific faults that they wish to keep track of in their management system.

38> As to claim 35, Lim and Hutcheson do not explicitly disclose providing a topology module.

39> Rangarajan discloses providing a topology module configured to display at least a graphical representation of network elements and connections between said network elements [Figure 9 «item 905» | column 6 «lines 27-36» | column 7 «lines 21-24»]. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's topology module into Lim's management system to allow users to more clearly see a map of the configuration of network resources in the network. One would have been motivated to perform such an implementation as such a map would allow users to more effectively manage the network resources.

40> As to claim 36, Lim and Hutcheson do not explicitly disclose storing a topology map sub-filter.

41> Rangarajan discloses storing a topology map sub-filter of the display filter, said topology map sub-filter configured to identify which of said network elements and network element connections to include in said topology map [Figure 9 «item 905» | column 6 «lines 27-36» | column 7 «lines 21-24 and 37-61»]. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's topology sub-filter into Lim's management system to allow users to control over what network devices are seen on a map of the network. One would have been motivated to perform such an implementation as such a map would allow users to more effectively manage the network resources.

42> As to claims 46 and 48-51, as they are merely systems that implement the steps of the method of claims 31 and 33-36, they do not teach or further define over the claimed limitations. Therefore, claims 46 and 48-51 are rejected for the same reasons as set forth for claims 31 and 33-36, supra.

43> Claims 21, 22, 26-28, 30, 32, 37-39, 41-43, 45, 47, 52 and 53 are rejected under 35 U.S.C § 103(a) as being unpatentable over Dobbins et al, U.S Patent Publication No. 2002|0066033 ["Dobbins"], in view of Lim.

44> As to claim 21, Dobbins discloses a method for filtering on-line service information provided through a management portal to a customer of customized network services provided by resources of a service provider network, comprising:

applying to said service provider network a security filter definable by service provider and not the customer, said security filter corresponding to the customer and specifying the network resources allocated to that customer [0009, 0024, 0043 where : Dobbins discloses policies controllable by the administrator that determine which content and network resources a particular subscriber has access];

applying a display filter to resources of the service provider network not excluded by said security filter, said display filter specifying network resources for which the on-line service information is desired by the customer [0023, 0024, 0026 : after applying the authentication policy, Dobbins' system applies the subscriber's profile to further refine which content and services that the user desires]; and

executing at least one management information module to generate a portal display of on-line service information, wherein said at least one management information module operates only on those network resources of said service provider network which have not been excluded by said security filter and said display filter [0025, 0036, 0037 where : Dobbins' renderer delivers a portal containing the data and content refined by the user policies].

Dobbins does disclose a service provider network, but does not to expressly disclose the service network or the resources are included in a partitioned network.

45> In a similar field of invention, Lim is directed towards a system enabling a service provider to manage its services partition its network resources into different networks associated with different customers [column 1 «lines 37-62» | column 20 «lines 61-62»]. Lim discloses network resources of a partitioned network allocated to a customer with the partitioned network including at least a portion of said service provider network [column 25-29» | column 21 «lines 28 and 46-64» | column 22 «lines 24-40»]. It would have been obvious to one of ordinary skill in the art to modify Dobbins to include the partitioned networks as taught by Lim. Lim discloses that partitioned networks are well known in the art for network management systems [column 1 «lines 37-62»]. The partitioned networks would improve Dobbins by providing a service provider the ability to divide network resources and allocate them to customers.

46> As to claim 22, Dobbins discloses applying a customer sub-filter to provide an association of said corresponding customer and said network resources contained in said partitioned network allocated to the customer [0009, 0024, 0037, 0043].

47> As to claim 26, Dobbins discloses a method for filtering on-line service information presented through a management portal to a customer of customized network services provided by resources of a service provider network, comprising:

storing, in a configuration database accessible by a service provider and not the customer, security filters each specifying network resources of a partitioned network allocated to a corresponding customer [0010, 0017, 0023];

providing a plurality of modules each configured to provide a respective portal display of on-line service information [0021, 0024, 0027];

storing, in a filter library accessible to the customer, display filters each configured to specify customer-selected network resources to which selected ones of said plurality of modules it to be applied [0010, 0017, 0023, 0036];

displaying a portal display of on-line service information generated from application of one of said plurality of modules to network resources resulting from application to the service provider network of a security filter corresponding to the customer and at least one said display filters [0009, 0010, 0017, 0023, 0036, 0037].

Dobbins does not expressly disclose partitioning the service provider network into a plurality of partitioned networks nor does he disclose allocating one of said partitioned networks to the customer.

48> Lim discloses partitioning the service provider network into a plurality of partitioned networks nor does he disclose allocating one of said partitioned networks to the customer [column 1 «lines 37-62» | column 25-29» | column 21 «lines 28 and 46-64» | column 22 «lines 24-40»]. It would have been obvious to one of ordinary skill in the art to modify Dobbins to include the partitioned networks as taught by Lim. Lim discloses that partitioned networks are well known in the art for network management systems [column 1 «lines 37-62»]. The partitioned networks would improve Dobbins by providing a service provider the ability to divide network resources and allocate them to customers.

49> As to claim 27, as it is does not teach or further define over previously claimed limitations, it is similarly rejected for at least the same reasons set forth for claim 22.

50> As to claim 28, Dobbins discloses a customer sub-filter that is configured to filter on at least one of a node level and interface level of said service provider network [Figure 1 | 0110].

51> As to claim 30, Dobbins discloses specifying an internet protocol interface sub-filter of said security filter, said IP interface sub-filter configured to filter on an IP address of a network device [0022].

52> As to claim 32, Dobbins discloses the method of claim 26 further comprising specifying an interface selection sub-filter of said display filter, said interface selection sub-filter configured to filter one of a set of at least one network interfaces [0052].

53> As to claim 37, Dobbins discloses providing a network health module configured to display a status or health report network resources to which said network health module is applied [0028].

54> As to claim Dobbins discloses storing a network health sub-filter of the display filter, said network health sub-filter configured to identify which of said network elements to monitor for said status and health report [0028, 0133].

55> As to claim 39, Dobbins discloses invoking said security filter by parsing a customer record in said user configuration database [0027, 0028].

56> As to claim 40, Dobbins discloses invoking said display filter by invoking said selected module [0053].

57> As to claims 41-43, 45, 47, 52 and 53, as they are merely systems that implement the steps of the method of claims 26-28, 30, 32, 37 and 38, they do not teach or further define over the claimed limitations. Therefore, claims 41-43, 45, 47, 52 and 53 are rejected for the same reasons as set forth for claims 26-28, 30, 32, 37 and 38, supra.

58> Claims 29 and 44 are rejected under 35 U.S.C § 103(a) as being unpatentable over Dobbins and Lim, in further view of Teijido et al, U.S Patent No. 2002|0053020 ["Teijido"].

59> As to claim 29, Dobbins and Lim do disclose utilizing sub-filters [see Hutcheson, 0143, 0164 : privilege filters accessible resources, profile further refines accessible resources to ones of interest to the user] but do not explicitly disclose specifying an internet protocol host sub-filter of said security filter, said IP host sub-filter configured to filter on a network name of a network device.

60> Teijido discloses an internet protocol host sub-filter of said security filter, said IP host sub-filter configured to filter on a network name of a network device [0049, 0070 : "...limit access to only a predefined specific set of client machines."; "...host id"]. It would have been obvious to one of ordinary skill in the art to incorporate Teijido's host sub-filter into Dobbins' management system to provide a level of security in accessing and viewing network resources. Such an implementation would ensure that the data can be tailored to a specific set of client machines.

61> As to claim 44, as it does not teach or further define over the previously claimed limitations, it is rejected for the reasons set forth for claim 29, supra.

62> Claims 23-25, 31, 33-36, 46 and 48-51 are rejected under 35 U.S.C § 103(a) as being unpatentable over Dobbins and Lim, in further view of Rangarajan et al, U.S Patent No. 6.275.225, ["Rangarajan"].

63> As to claim 23, Dobbins and Lim do not explicitly disclose an alarm module.

64> Rangarajan discloses an alarm module configured to display information regarding alarm conditions occurring in said non-excluded resources [Figure 5 «item 509» | column 5 «lines 50-53» | column 10 «lines 6-10» : wherein the devices correspond to network resources and clients are only able to work with resources that have been assigned to them (excluded resources)]. Furthermore, Lim discloses resources that can only be utilized by customers with the property authority. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's alarm module into Dobbins' management system to allow users to select nodes that would enable monitoring of alarm conditions in the network resources to which they only have access. One would have motivated to perform such an implementation enable users to more efficiently manage resources.

65> As to claim 24, Dobbins and Lim do not explicitly disclose a topology module configured to display at least a graphical representation of network elements and connections between said network elements included in said non-excluded network resources.

66> Rangarajan discloses providing a topology module configured to display at least a graphical representation of network elements and connections between said network elements [Figure 9 «item 905» | column 6 «lines 27-36» | column 7 «lines 21-24»]. Furthermore, Lim discloses resources that can only be utilized by customers with the property authority. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's topology module into Dobbins' management system to allow users to more clearly see a map of the configuration of network resources to which they only have access in the network. One would have been motivated to perform such an implementation as such a map would allow users to more effectively manage the network resources.

67> As to claim 25, Dobbins' and Lim do not explicitly disclose a network health module configured to display a status or health report of said non-excluded network resources.

68> Rangarajan discloses a network health module configured to display a status or health report of said non-excluded network resources [Figure 9 «item 907» : "critical, major, minor.."]. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's health module into Lim's data access system to allow users to keep track and remotely monitor network resources as needed.

69> As to claim 31, Dobbins and Lim do disclose utilizing sub-filters [see Dobbins, applying the security filter to the user, the applying a profile filter based on user preferences], but do not explicitly disclose a node selection sub-filter.

70> Rangarajan discloses a node selection sub-filter of said display filter, said node selection sub-filter configured to filter on network nodes of the service provider network [column 6 «lines 27-33» | column 7 «lines 10-14»]. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's node filtering functionality into Dobbins' management system to enable users to manage network devices through a user selected view of the nodes in the network.

71> As to claim 33, Dobbins and Lim do not explicitly disclose an alarm module.

72> Rangarajan discloses an alarm module configured to display alarm conditions in network resources to which said alarm module is applied [Figure 5 «item 509» | column 10 «lines 6-10» : wherein the devices correspond to network resources]. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's alarm module into Dobbins' management system to allow users to select nodes that would enable monitoring of alarm conditions in the network resources. One would have motivated to perform such an implementation enable users to more efficiently manage resources.

73> As to claim 34, Dobbins and Lim do not explicitly disclose an alarm sub-filter.

74> Rangarajan discloses storing an alarm sub-filter of the display filter, said alarm sub-filter providing filtering capability of a display of alarm categories [column 6 «lines 27-36» | column 7 «lines 37-61»: "selected fault list"]. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's alarm sub-filter into Dobbins' management system to enable users to select specific faults that they wish to keep track of in their management system.

75> As to claim 35, Dobbins and Lim do not explicitly disclose providing a topology module.

76> Rangarajan discloses providing a topology module configured to display at least a graphical representation of network elements and connections between said network elements [Figure 9 «item 905» | column 6 «lines 27-36» | column 7 «lines 21-24»]. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's topology module into Dobbins' management system to allow users to more clearly see a map of the configuration of network resources in the network. One would have been motivated to perform such an implementation as such a map would allow users to more effectively manage the network resources.

77> As to claim 36, Dobbins and Lim do not explicitly disclose storing a topology map sub-filter.

78> Rangarajan discloses storing a topology map sub-filter of the display filter, said topology map sub-filter configured to identify which of said network elements and network element connections to include in said topology map [Figure 9 «item 905» | column 6 «lines 27-36» | column 7 «lines 21-24 and 37-61»]. It would have been obvious to one of ordinary skill in the art to incorporate Rangarajan's topology sub-filter into Dobbins' management system to allow users to control over what network devices are seen on a map of the network. One would have been motivated to perform such an implementation as such a map would allow users to more effectively manage the network resources.

79> As to claims 46 and 48-51, as they are merely systems that implement the steps of the method of claims 31 and 33-36, they do not teach or further define over the claimed limitations. Therefore, claims 46 and 48-51 are rejected for the same reasons as set forth for claims 31 and 33-36, supra.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dohm Chankong whose telephone number is 571.272.3942. The examiner can normally be reached on Monday-Thursday [7:00 AM to 5:00 PM].

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on 571.272.3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DC

BUNJOB JAROENCHONWANIT
PRIMARY EXAMINER